

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-032216

(43)Date of publication of application : 31.01.2002

(51)Int.CI.

G06F 9/06

G06F 15/00

(21)Application number : 2000-218325

(71)Applicant : FUJITSU LTD

(22)Date of filing : 19.07.2000

(72)Inventor : KATSUKAWA YASUSHI
YAMAZAKI TOSHIYA

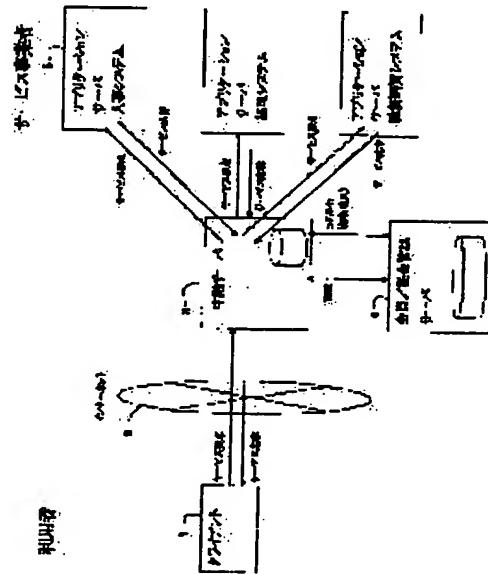
(54) HOSTING DEVICE FOR APPLICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a hosting device by which a service company of application can start service at low cost and in short time and a user of the service can be authenticated and charged in common for plural kinds of application service.

SOLUTION: The service company 5 having various application servers are registered in a relay server 3 and the relay server is accessed first when a client 1 uses the service to be offered by the service company 5. The client 1 is authenticated and connected to the service company 5 at the relay server 3. Also the use of the service by the client 1 is charged at the relay server 3. Therefor, a member/charging management server 4 is connected to and a necessary database is provided in the relay server 3.

本発明の実施形態における認証及び
課金処理のシステム構成を示す図



LEGAL STATUS

[Date of request for examination] 25.11.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-32216

(P2002-32216A)

(43)公開日 平成14年1月31日 (2002.1.31)

(51)Int.Cl.
G 0 6 F 9/06
15/00

識別記号
Z E C
3 1 0

F I
G 0 6 F 9/06
15/00

テマコト[®] (参考)
Z E C 5 B 0 7 6
3 1 0 D 5 B 0 8 5

(21)出願番号 特願2000-218325(P2000-218325)

(22)出願日 平成12年7月19日 (2000.7.19)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 勝川 康史

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 山崎 利哉

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100074099

弁理士 大曾 義之 (外1名)

F ターム(参考) 5B076 FB20 FC10

5B085 AC04 AE23 BC01 BG07

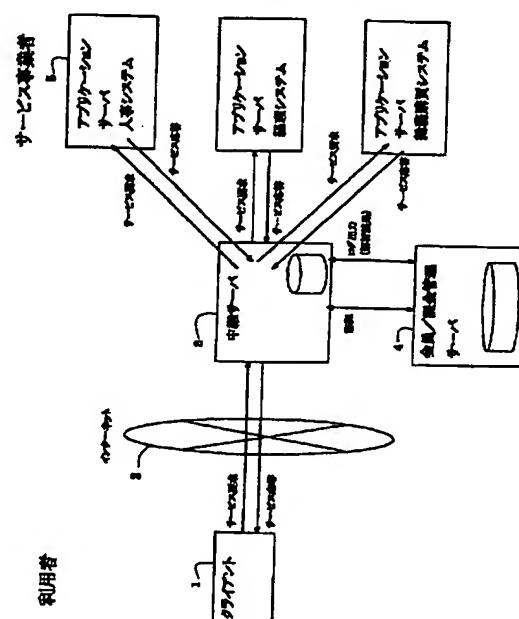
(54)【発明の名称】 アプリケーションのホスティング装置

(57)【要約】

【課題】 アプリケーションのサービス事業者に対し、低成本かつ短期間でサービスを介し可能とし、サービスの利用者には複数のアプリケーションサービスに対し共通の認証及び課金を可能とするホスティング装置を提供する。

【解決手段】 様々なアプリケーションサーバ有するサービス事業者5は、中継サーバ3に登録し、クライアント1がサービス事業者5の提供するサービスを利用する場合には、中継サーバ3に最初にアクセスする。中継サーバ3では、クライアント1を認証し、サービス事業者5に接続する。また、クライアント1のサービス利用に対する課金も中継サーバ3において行う。このため、中継サーバ3には、会員/課金管理サーバ4が接続され、必要なデータベースを設ける。

本発明の実施形態における認証及び
課金処理のシステム構成を示す図



【特許請求の範囲】

【請求項1】クライアントと、アプリケーションサーバによってアプリケーションサービスを提供するサービス業者とを仲介するホスティング装置であって、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証手段と、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納手段と、該認証用データ格納手段に格納されたデータに基づいて、該認証手段において認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログイン手段と、を備えることを特徴とするホスティング装置。

【請求項2】前記アプリケーションサーバによるアプリケーションサービスに対するアクセス権の設定において、ユーザをグルーピングし、グループ単位にサービスのアクセス権を設定することを特徴とする請求項1に記載のホスティング装置。

【請求項3】前記ユーザが前記ホスティング装置のポータルサイト(入り口)にアクセスすると、そのユーザが利用できるアプリケーションのURLメニューを表示することを特徴とする請求項1に記載のホスティング装置。

【請求項4】クライアントと、アプリケーションサーバによってサービスを提供するサービス業者とを仲介するホスティング方法であって、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証ステップと、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納ステップと、該認証用データ格納ステップで格納されたデータに基づいて、該認証ステップにおいて認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログインステップと、を備えることを特徴とするホスティング方法。

【請求項5】クライアントと、アプリケーションサーバによってサービスを提供するサービス業者とを仲介するホスティング方法を情報装置に実現させるプログラムを記録した記録媒体であって、該ホスティング方法は、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証ステップと、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納ステップと、該認証用データ格納ステップで格納されたデータに基づ

いて、該認証ステップにおいて認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログインステップと、を備えることを特徴とする情報装置読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アプリケーションのホスティングを行うホスティング装置に関する。

【0002】

【従来の技術】インターネットの普及、ネットワークインフラの整備に伴い、業務アプリケーションやパッケージソフトウェアなどのアプリケーションサーバの代行運用が急速に増加している。このような時流の中、アプリケーションを所有する事業者は、短期間でアプリケーションのホスティング対応ができる仕組みを望んでいる。また、利用者は、増加するアプリケーションのホスティングサービスを効率よく利用できる仕組みを望んでいる。

【0003】従来のアプリケーションのホスティングサービスでは、個々のアプリケーションサーバにおいて、利用者を識別するための認証処理を行い、課金を行なう際に必要な利用履歴などのログ情報を蓄積している。また、サービスの利用者はアプリケーション単位に認証手続きを行い、アプリケーション毎に利用分の課金明細を受領している。

【0004】

【発明が解決しようとする課題】アプリケーションのホスティングサービスを開始する場合、アプリケーションのサービス事業者は、アプリケーションに対して、認証や課金処理を実装する必要があり、そのための開発コスト、及び、開発期間が必要であった。また、アプリケーションのホスティングサービスの利用者は、アプリケーション毎に認証及び利用料金の支払いがあるため、複数のアプリケーションサービスを利用する場合には、その都度、異なるアカウントでの認証手続きの実行及び、複数の課金明細を受領するため、非効率かつ煩雑であった。

【0005】本発明の課題は、アプリケーションのサービス事業者に対し、低コストかつ短期間でサービスを介し可能とし、サービスの利用者には複数のアプリケーションサービスに対し共通の認証及び課金を可能とするホスティング装置を提供することである。

【0006】

【課題を解決するための手段】本発明のホスティング装置は、クライアントと、アプリケーションサーバによってアプリケーションサービスを提供するサービス業者とを仲介するホスティング装置であって、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証手段と、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該アプリケーションの認証システムを有している場合には、該アプリ

ケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納手段と、該認証用データ格納手段に格納されたデータに基づいて、該認証手段において認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログイン手段とを備えることを特徴とする。

【0007】本発明においては、クライアントとアプリケーションサーバとの間にホスティング装置としての中継サーバを設ける。中継サーバには、複数のアプリケーションサーバや複数のクライアントが接続される。中継サーバには、各アプリケーションサーバへのログイン情報が必要な場合に、中継サーバに登録した各ユーザ毎にログイン情報を保持し、ユーザが中継サーバへのログインが成功した後は、各アプリケーションサーバへのログインを自動的に行うようとする。従って、ユーザは、中継サーバにログインするだけで、全てのアプリケーションサーバを利用することが出来る。

【0008】また、アプリケーションサーバを有するサービス事業者においても、新規に中継サーバに登録するものだけではなく、既にサービスを行っており、独自の認証システムを有しているアプリケーションサーバも容易に中継サーバに収容することが出来る。すなわち、そのようなアプリケーションサーバにおいても、1回のログイン（中継サーバへの）だけでアプリケーションを利用できるようになる。

【0009】また、複数のアプリケーションサーバへのアクセスに対する課金を中継サーバにおいて一括して行うので、ユーザは自分のサービス利用状態の管理が簡単になり、また、サービス事業者は課金システムを自分のアプリケーションサーバに組み込む必要がないので、短期間でサービスの提供を始めることが出来る。

【0010】

【発明の実施の形態】本発明では、クライアントとアプリケーションサーバとの中間点に中継サーバを置き、個々のアプリケーションサーバで行う必要のあった認証及び課金処理を代行する。また、アプリケーションのホスティングサービス利用者を一元管理する事により、一つのアカウントで複数のアプリケーションサーバへの認証及び複数サービスの利用料金の請求を一本化した課金明細を作成する。

【0011】図1は、本発明の実施形態における認証及び課金処理のシステム構成を示す図である。図中、1はアプリケーションのホスティングサービス利用者の端末、2はネットワークとしてインターネット（他のネットワークでも適用可能なことは当然である。）、3は中継サーバ、4はアプリケーションのホスティングサービス利用者の一元管理及び中継サーバで出力した履歴ログを蓄積する会員／課金管理サーバ、5はサービス事業者のアプリケーションサーバである。

【0012】クライアント1がインターネット2を介し

て、中継サーバ3にサービス要求を出すと、中継サーバ3からクライアント1に認証画面が提示される。ここで、クライアント1からは、認証情報としてユーザIDやパスワードなどが入力され、中継サーバ3に返送される。中継サーバ3では、クライアント1から送られてきた認証情報に基づいて、クライアント1を使用するユーザの認証を行う。この際、中継サーバ3は、会員／課金管理サーバ4のデータベースを参照して、ユーザがホスティングサービスを利用するための会員であるか否かを検証する。ユーザが認証されると、サービス要求が各サービス事業者5に送信され、クライアント1には、各サービス事業者5が提供するアプリケーション画面が出力される。中継サーバ3では、ユーザの認証からユーザがどのようなサービスを中継サーバ3を介して受けたかをログとして取得し、会員／課金管理サーバ4のデータベースに当該ログを記録する。

【0013】サービス事業者5が提供するアプリケーションサービスとしては、人事システム、経理システム、総務購買システムなどが可能であるが、本発明はこれらに限定するものではない。

【0014】クライアント1がサービス事業者5のサービスからログオフするときは、中継サーバ3からもログオフすることになる。このログオフによってクライアント1の中継サーバ3を介したサービス利用が終了し、中継サーバ3のログの記録も終了する。そして、後に、中継サーバ3は、ログの記録内容を解析して、クライアント1のユーザがどのサービス事業者5のサービスをどの程度使用したかを算出し、課金情報を生成する。そして、この課金情報は、サービス利用明細としてクライアント1のユーザに送付される。中継サーバ3が課金情報を生成する場合には、サービス事業者5毎にどのようにクライアント1に課金するかを記録した、会員／課金管理サーバ4のデータベースを参照する。このように、ユーザの全てのサービス要求は中継サーバ3を通過するよう構成する。

【0015】図2は、サービス情報定義データのデータ構造を示す図である。まず、本実施形態のシステムによりアプリケーションのホスティングサービスを開始したいサービス事業者は、自アプリケーションサーバで提供するサービスを中継サーバのデータベースに図2のデータ構造で定義する。サービス情報定義データの登録の仕方は、従来のネットワークを介したデータの入力手法を採用すればよい。

【0016】このサービス情報定義データにおいては、認証及び課金対象とするサービス毎に、サービス名、サービスを提供するホームページのURL、個別認証の有無、及び料金プランや料金体系などの課金情報を定義する。例えば、図2の例においては、人事システムのサービス提供は、URLが「www.foo.jp/sv0001-1, www.foo.jp/sv0001-2」のホームページにおいて行われ、個別認

証（アプリケーション側での認証）が不要（無）であり、料金プランは「固定」で、月額200円となっている。その他のサービスについても同様である。中継サーバにおいて認証処理をバイパスする場合には、認証不要とするURLを定義するようにしても良い。

【0017】また、本実施形態のシステムを利用したい利用者は中継サーバに対して会員登録を行う。図3は、利用者クライアント機器の種別定義のデータ構造を示した図である。

【0018】図3においては、利用者としてuser0001・user0004～が登録されており、クライアント種別として、user0001は携帯電話であり、user0002～user0004は、一般的PCであることが登録されている。

【0019】また、利用者（ユーザ）の登録に際しては、各ユーザをグループ化し、グループ毎に利用できるサービスを定義するようにしても良い。図4は、利用者グループ情報定義データの構造であり、図5は、グループ単位でのアクセス権限情報定義データの構造である。

【0020】図4においては、利用者として、user0001～user0004～が登録されており、user0001とuser0002～user0004が同じgroup001にグループ分けされている。user0003とuser0004とは、それぞれ、group002、group003にグループ分けされている。

【0021】図5においては、それぞれのグループに対して、アクセス可能URLとアクセス不可能URLが設定されており、group001においては、www.foo.jp/sv0001-1と、www.foo.jp/sv0002/d1がアクセス可能URLとして設定されている。また、group001のアクセス不可能URLは、www.foo.jp/sv002が設定されている。group002のアクセス可能URLは、www.foo.jp/sv0001-2であり、アクセス不可能URLは存在しない。group003においては、アクセス可能URLがwww.foo.jp/sv0002であり、アクセス不可能URLは、www.foo.jp/sv0002/d1となっている。

【0022】従って、図4と図5を合わせて考えると、user0001、user0002は、www.foo.jp/sv0001-1と、www.foo.jp/sv0002/d1にアクセス可能であるが、www.foo.jp/sv002はアクセス不可能となっている。user0003、user0004についても同様である。

【0023】図6は、アプリケーションサーバの個別認証情報を示すデータ構造である。アプリケーションサーバで個別の認証手続きを行う場合には、図6のデータ構造で個別認証情報を定義する。

【0024】例えば、図6において、user0001が総務購買システムのサービスを利用する時は、総務購買システムのサーバ側で個別の認証が行われ、このときに使用されるuser0001の認証情報は、ユーザIDが「vp0001」、パスワードが「xxxxxx」であり、認証方法が「BASIC認証」である旨が登録されている。ここで、BASIC認証とは、現在のWWW（World Wide Web）における標準認

証方式のことである。図6においては、同様にuser0002についても登録がされている。

【0025】図6のアプリケーションサーバ個別認証情報が設定されている場合には、中継サーバは、ユーザからのサービス要求に従って、中継サーバの認証を終えると、次に、図6のアプリケーションサーバ個別認証情報を参照して、アプリケーションサーバ側で当該ユーザの認証に必要なユーザIDやパスワードを設定された認証方法に従って送信し、ユーザが自分でアプリケーションサーバへの認証情報を入力しなくとも自動的に個別認証を行う。

【0026】このように、個別認証のための構成を設けるのは、中継サーバが提供するホスティングサービスに、既に稼働中のアプリケーションサーバが加入する場合、当該アプリケーションサーバは、既に独自の認証／課金システムを備えている可能性が高なので、何もしないと、利用者は、中継サーバの認証を行った後、アプリケーションサーバにアクセスする際に再度別個に認証を受けなければならない。このような不便をなくすために、中継サーバ側で、アプリケーションサーバにログインするために必要なデータを保持しておき、中継サーバにログインするだけで、どのアプリケーションサーバにもアクセスできるようにするものである。もちろん、新規に中継サーバが提供するホスティングサービスに加入するアプリケーションサーバは、独自に認証／課金システムを備える必要はなく、従って、中継サーバでは、個別認証のためのデータを保持する必要はない。

【0027】以上説明したように、サービス情報、会員情報、グループ情報、アクセス権限情報及びアプリケーションサーバ個別認証情報は、会員／課金管理サーバのデータベースにおいて一元管理する。

【0028】図7は、ログイン画面の表示例を示す図である。利用者は、アプリケーションサーバの提供するサービスを利用したい時、クライアント1からサービスの要求先を含むサービス要求を送信する。中継サーバ3はクライアント1からのサービス要求を受け付け、アカウント情報を取り出す。利用者アカウントが無い場合には、要求先のURLが認証不要かを判定する。認証不要の場合には、アプリケーションサーバ6にサービス要求を転送する。認証要の場合には、利用者アカウントを受け取るために、図7の画面例で示すログイン画面をクライアント1に表示する。このとき、通信プロトコルがHTTPの場合には、BASIC認証のログイン画面を表示しても良い。

【0029】サービス要求内に利用者アカウントがある場合には、アカウント情報を取り出し、会員／課金管理サーバ4上の登録情報と照合する。正規登録利用者でない場合には、要求先のURLが認証不要か否かを判定する。認証不要の場合には、アプリケーションサーバ6にサービス要求を転送する。認証要の場合には、アクセス

を拒否する。

【0030】正規登録利用者の場合に、サービス要求内容がメニュー表示依頼ならば、利用者がアクセス可能なサービスをアクセス権限情報から検索し、図8で示す表示メニューを作成し、クライアント1に表示する。メニュー表示依頼以外のサービス要求で有れば、次にアクセス権限の判定処理を行う。

【0031】上述したように、図8は、表示メニューの表示例を示している。図8(a)は、user0001、user002のASP(Application Service Provider)サービスメニューの表示例を示している。user0001とuser0002は、図4が示すように、group0001に属しており、図5と図2から明らかなように、人事システムと総務購買システムの利用が可能となっている。同様に、図8(b)に示すように、user0003は、人事システムが、また、図8(c)が示すように、user0004は、経理システムが利用可能となっている。

【0032】図9は、ユーザが中継サーバを介してアプリケーションサーバにサービス要求を行う場合のシーケンスを示す図である。図9においては、user0001が人事システム、及び総務購買システムを利用する場合のシーケンスを示している。

【0033】まず、クライアントである利用者user0001から人事システムへのサービス要求を送信する。このサービス要求は中継サーバによって受信される。今の場合、user0001は、中継サーバへの初回アクセスを行っているので、中継サーバは、user0001に対し、ログイン画面を表示する。user0001は、ユーザID、パスワードを入力し、中継サーバに送信する。中継サーバで認証が成功すると、サービス要求をサービス事業者の人事システムに送信する。人事システムでは、中継サーバからのサービス要求に対し、中継サーバにサービス応答を行いサービスを提供するコンテンツを送信する。中継サーバは、人事システムからコンテンツを受け取ると、user0001のアクセス不可能URLやuser0001の利用端末機種などを参照して、人事システムの表示コンテンツの内から、アクセス不可能URLへのリンクを削除したり、携帯電話用画面に変換するなどのコンテンツ変換を実行し、該変換されたコンテンツをuser0001に送信することによってサービス応答を行う。これにより、user0001は、人事システムを利用可能となる。

【0034】次に、user0001が別のサービス事業者の提供する総務購買システムを利用しようとする場合は、user0001側から中継サーバに総務購買システムへのサービス要求を送信する。中継サーバは、総務購買システムが個別認証を必要とすることをデータベースから取得すると、user0001の個別認証に必要なユーザIDやパスワードを認証方法に従って、総務購買システムに送信し、個別認証代行処理を実行すると共に、総務購買システムにサービス要求を行う。総務購買システムでは、個別認証

に成功すると、サービス応答を中継サーバに送信する。サービス応答を受け取った中継サーバは、前述したようなコンテンツの変換を行い、user0001に対し、サービス応答を行う。このようにして、user0001は、総務購買システムのサービスも利用することが出来るようになる。

【0035】図10は、中継サーバの初回のサービス要求受付からアプリケーションサービスの提供開始までの処理を示すフローチャートである。まず、ステップS1において、初回のサービス要求を受け付ける。次に、ステップS2において、利用者判定処理を行う。利用者判定処理については詳細は後述する。次に、ステップS3において、アクセス権限判定処理を行う。アクセス権限判定処理についても後述する。そして、ステップS4において、アプリケーションサーバの個別認証処理を行う。もちろん、アプリケーションサーバが個別認証を必要としない場合には、特に処理はしない。そして、ステップS5において、アプリケーションサーバにサービス要求を転送し、ステップS6において、利用ログを出力する。

【0036】図11は、図10の利用者判定処理の詳細を示すフローチャートである。まず、ステップS10において、利用者アカウントをサービス要求から取り出す。そして、ステップS11において、利用者アカウントが取り出せたか否か、すなわち、利用者アカウントとして有効なものがサービス要求に含まれていたか否かを判断する。利用者アカウントがない場合には、ステップS12において、利用者が利用しようとするアプリケーションサーバが認証を必要とするものか否かを判断する。認証が不要の場合には、ステップS13において、アプリケーションサーバにサービス要求を転送する。ステップS12において、認証が必要と判断された場合には、ステップS14において、利用者にログイン画面を提示し、利用者アカウントを受け取る。そして、ステップS10に戻って処理を繰り返す。

【0037】ステップS11において、利用者アカウントが得られたと判断された場合には、ステップS15において、会員/課金管理サーバ上の登録情報と照合し、ステップS16において、正規登録利用者か否かを判断する。ステップS16において、正規登録利用者でないと判断された場合には、ステップS17において、利用者がアクセスしようとしているアプリケーションサーバは、認証を必要としているか否かを判断する。認証が不要の場合には、ステップS18に進んで、アプリケーションサーバにサービス要求を転送して処理を終了する。ステップS17において、認証が必要と判断された場合には、アクセスを拒否する。

【0038】ステップS16において、アクセスしてきた利用者が正規登録利用者であると判断された場合には、ステップS19において、利用者からのサービス要求がメニュー表示要求か否かを判断し、メニュー表示要

求である場合には、ステップS20において利用者メニューを生成出し、処理を終了する。ステップS19において、サービス要求が利用者メニュー表示でないと判断された場合には、利用者判定処理が終了したとして、この処理フローから抜ける。

【0039】図12は、図10のアクセス権限判定処理の詳細を示すフローチャートである。まず、ステップS30において、サービス要求に含まれる要求先URLを取り出す。ステップS31において、取り出したURLと、アクセス権限情報のURLリストと比較し、ステップS32において、URLリスト内に要求URLがあるか無いかを判断する。無い場合には、アクセス拒否を行う。ステップS32において、要求URLがURLリストにあった場合には、ステップS33において、サービス要求を要求してきた利用者が利用可能なURLであるか否かを判断し、利用不可である場合には、アクセス拒否をし、利用可である場合には、アクセス権限判定処理を終了したとして、この処理フローから抜ける。

【0040】図13は、中継サーバがアプリケーションサーバからサービス応答を受け取った際の処理を示すフローチャートである。まず、ステップS40において、サービス応答を受信すると、ステップS41において、利用者の機器（クライアント）は一般のPCか否かを判断する。クライアントが一般のPCの場合には、ステップS43において、クライアントにサービス応答を転送する。ステップS41において、クライアントが一般のPCではないと判断された場合には、ステップS42において、コンテンツを携帯電話などの小型機器用表示にコンテンツを変換して、ステップS43において、クライアントにサービス応答を転送する。

【0041】なお、ここでは、コンテンツ変換のトリガとして、クライアントが一般PCか否かのみを判断するように示したが、その他の要素を考慮してもよく、例えば、前述したように、利用者がアクセス不可能なURLへのリンクがコンテンツの中に含まれているか否かを判断し、含まれている場合には、このリンクを取り除く変換をしてクライアントにサービス応答の転送を行うようにしても良い。

【0042】以上説明したように、中継サーバは、図2に示すアクセス権限の判定処理では、中継サーバは、クライアントからのサービス要求からサービスの要求先URLを取り出すと会員/課金管理サーバ4上のアクセス権限情報と照合する。このとき、アクセス権限情報は中継サーバ上にキャッシュしておいても良い。アクセス権限の判定の結果、アクセス権限がある場合には、図6のアプリケーションサーバ個別認証情報を参照し、アプリケーションサーバに個別の認証があるか確認する。個別の認証がない場合には、要求先のサービスを所有するアプリケーションサーバにサービス要求を転送する。個別の認証処理がある場合には、個別認証情報に従い、そ

の認証手続きを代行実行し、その後、要求先のサービスを所有するアプリケーションサーバにサービス要求を転送する。アプリケーションサーバにサービス要求を転送した際には、中継サーバ上に履歴ログを出力する。履歴ログはその後、会員/課金管理サーバに転送し課金計算を行った後、図14のデータ構造の課金明細を作成する。このとき、履歴ログは直後、会員/課金管理サーバ4上に出力しても良い。

【0043】中継サーバはサービス要求転送後、アプリケーションサーバからのサービス応答を受信する。このとき、利用者のクライアント種別を判定し、一般PCでない場合には、その利用機器で閲覧できる形式にコンテンツを変換後、サービス応答を転送する。

【0044】ここで、上述した図14は、課金明細の例である。本実施形態の課金明細では、各利用者（ユーザ）毎に、どのアプリケーションサーバを何円分使用したかが示されると共に、各ユーザ毎の合計の課金額が算出される。従来では、各アプリケーションサーバが独自に認証及び課金システムを有していたため、複数のアプリケーションサーバを利用すると、利用者には、複数のアプリケーションサーバからそれぞれの明細が送られてくることになる。しかし、本実施形態によれば、同一中継サーバを介して行われたサービスは、一括して課金処理されるので、複数のアプリケーションサーバを使用しても、これらは、まとめられた形で明細に記載され、合計利用金額が算出されて利用者に通知される。従つて、アプリケーションサーバを有するサービス事業者は、中継サーバの提供するホスティングサービスに参加することにより、自分で課金処理を行わなくて良いので、サービス提供のために必要とされる投資が少なくて済む。また、利用者は、自分の利用したサービスが一括して課金されるので、自分がどのサービスをどの程度利用したかの管理がしやすくなる。

【0045】なお、上記実施形態においては、中継サーバが単一の場合について説明したが、複数の中継サーバを介して、アプリケーションサーバに接続する形態をとっても良い。ただし、認証及び課金を一括して行うために、認証情報と課金情報を格納するデータベースは、上記複数の中継サーバに共通に設けるようにする。

【0046】図15は、本発明の実施形態の中継サーバ及び会員/課金管理サーバの機能をプログラムで実現しようとする場合に要求されるハードウェア環境の例を示す図である。

【0047】CPU11は、バス10を介して、ROM12、RAM13、通信インターフェース14、記録装置17、記録媒体読み取り装置18、入出力装置20に接続される。本発明の実施形態を実現するプログラムは、ROM12、記録装置17、可搬記録媒体19に記録される。また、各種データベースは、記録装置17あるいは、可搬記録媒体19に記録される。記録装置17

は、例えば、ハードディスクであり、可搬記録媒体19は、例えば、CD-ROM、フロッピー（登録商標）ディスク、DVDなどである。可搬記録媒体19に記録されたプログラムあるいは、データは、記録媒体読み取り装置18を介して、記録装置17からRAM13に展開され、CPU11が実行可能な状態とされる。記録媒体読み取り装置18や記録装置17、あるいは、図15の情報装置の管理人が該情報装置を制御する際に使用する入出力装置20、及び通信インターフェース14をCPU11が制御可能するために、ROM12には、BIOSなどの基本プログラムが格納される。基本プログラムは同図の情報装置が電源投入された時点で実行される。入出力装置20は、例えば、ディスプレイ、キーボード、マウスなどからなる。

【0048】また、本発明の実施形態を実現するプログラムは、通信インターフェース14を使った通信によって、ネットワーク15を介して、情報提供者16からダウンロードして実行しても良い。また、各種データベースを可搬記録媒体19や記録装置17に構築せず、情報提供者16の有するデータベースに格納するようにしても良い。また、本発明の実施形態を実現するプログラムをダウンロードするのではなく、情報提供者16とネットワーク15で接続したまま、いわゆるネットワーク環境下の下に当該プログラムを実行して、本発明の実施形態を実現しても良い。

＜付記＞

（付記1）クライアントと、アプリケーションサーバによってアプリケーションサービスを提供するサービス業者とを仲介するホスティング装置であって、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証手段と、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納手段と、該認証用データ格納手段に格納されたデータに基づいて、該認証手段において認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログイン手段と、を備えることを特徴とするホスティング装置。

（付記2）ユーザ毎に、該ユーザが利用可能なサービスのリストを有し、クライアントからのサービス要求時に該リストと該クライアントのユーザの識別情報を照合することにより該ユーザが該サービスにアクセスする権利を有するか否かを判定することを特徴とする付記1に記載のホスティング装置。

（付記3）1つの共通ログイン情報を用いて、複数のアプリケーションサーバへの認証を行うことを特徴とする付記1に記載のホスティング装置。

（付記4）更に、該ユーザが該アプリケーションサーバによるサービスを利用した場合に、該ユーザへの課金を行う課金手段を備え、ユーザ毎に複数のアプリケーショ

ンサービスの利用料金の請求を一本化した課金明細を作成することを特徴とする付記1に記載のホスティング装置。

（付記5）前記アプリケーションサーバによるアプリケーションサービスに対するアクセス権の設定において、ユーザをグループ化し、グループ単位にサービスのアクセス権を設定することを特徴とする付記1に記載のホスティング装置。

（付記6）前記ユーザが前記ホスティング装置のポータルサイト（入り口）にアクセスすると、そのユーザが利用できるアプリケーションのURLメニューを表示することを特徴とする付記1に記載のホスティング装置。

（付記7）クライアントと、アプリケーションサーバによってサービスを提供するサービス業者とを仲介するホスティング方法であって、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証ステップと、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納ステップと、該認証用データ格納ステップで格納されたデータに基づいて、該認証ステップにおいて認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログインステップと、を備えることを特徴とするホスティング方法。

（付記8）クライアントと、アプリケーションサーバによってサービスを提供するサービス業者とを仲介するホスティング方法を情報装置に実現させるプログラムを記録した記録媒体であって、該ホスティング方法は、該クライアントを使用するユーザ情報に基づいて、該クライアントのユーザを認証する認証ステップと、該アプリケーションサーバが独自の認証システムを有している場合には、該アプリケーションサーバに該ユーザがログインするために必要なデータを格納する認証用データ格納ステップと、該認証用データ格納ステップで格納されたデータに基づいて、該認証ステップにおいて認証が成功したユーザの該アプリケーションサーバへのログインを自動的に行う自動ログインステップと、を備えることを特徴とする情報装置読み取り可能な記録媒体。

【0049】

【発明の効果】本発明によれば、アプリケーションのホスティング事業を開始するサービス業者が、個別に認証及び、課金処理をアプリケーションサーバ上に実装する必要が無くなるため、その分の開発コストを削減でき、また、サービス開始までの期間を短縮できる。また、利用者にとっても、これまでアプリケーション毎に異なるアカウントでの認証手続きの実行及び、複数の課金明細を受領していたものが、一つの共通アカウントによるシングルサインオン及び、複数のサービスの利用料金の請求を一本化できる課金明細を受領できるため、効率よく

サービスを利用できるようになる。

【図面の簡単な説明】

【図1】本発明の実施形態における認証及び課金処理のシステム構成を示す図である。

【図2】サービス情報定義データのデータ構造を示す図である。

【図3】利用者クライアント機器の種別定義のデータ構造を示した図である。

【図4】利用者グループ情報定義データの構造である。

【図5】グループ単位でのアクセス権限情報定義データの構造である。

【図6】アプリケーションサーバの個別認証情報を示すデータ構造である。

【図7】ログイン画面の表示例を示す図である。

【図8】表示メニューの表示例を示す図である。

【図9】ユーザが中継サーバを介してアプリケーションサーバにサービス要求を行う場合のシーケンスを示す図である。

【図10】中継サーバの初回のサービス要求受付からア

プリケーションサービスの提供開始までの処理を示すフローチャートである。

【図11】図10の利用者判定処理の詳細を示すフローチャートである。

【図12】図10のアクセス権限判定処理の詳細を示すフローチャートである。

【図13】中継サーバがアプリケーションサーバからサービス応答を受け取った際の処理を示すフローチャートである。

【図14】課金明細の例を示す図である。

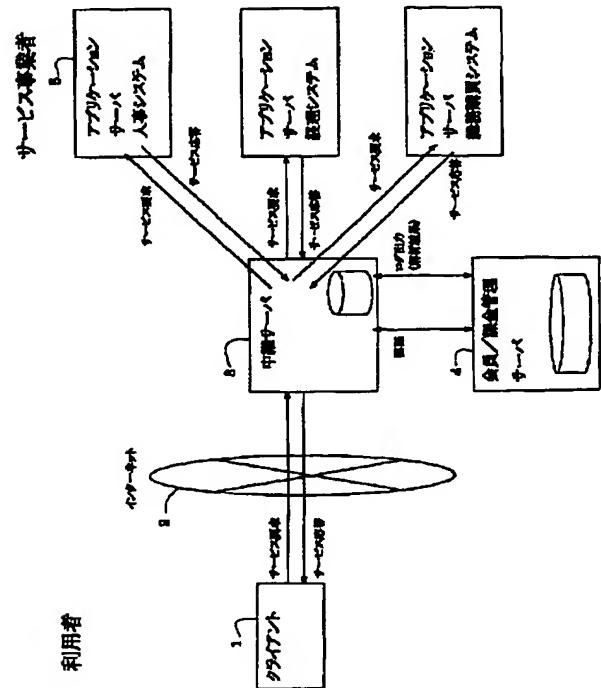
【図15】本発明の実施形態の中継サーバ及び会員/課金管理サーバの機能をプログラムで実現しようとする場合に要求されるハードウェア環境の例を示す図である。

【符号の説明】

- 1 クライアント
- 2 インターネット
- 3 中継サーバ
- 4 会員/課金管理サーバ
- 5 サービス業者

【図1】

本発明の実施形態における認証及び
課金処理のシステム構成を示す図



【図3】

利用者クライアント機器の種別定義の
データ構造を示した図

利用者	クライアント種別
user0001	携帯電話
user0002	一般PC
user0003	一般PC
user0004	一般PC
:	:

【図2】

サービス情報定義データのデータ構造を示す図

サービス名	URL	個別認証	料金プラン	料金
人事システム	www.foo.jp/sv0001-1, www.foo.jp/sv0001-2	無	固定	200円/月
経理システム	www.foo.jp/sv0002	無	従量	10円/単位
総務購買システム	www.foo.jp/sv0002/d1	有	固定	100円/月
認証不要	www.foo.jp/sv004, www.foo.jp/sv005	—	—	—
:	:	:	:	:

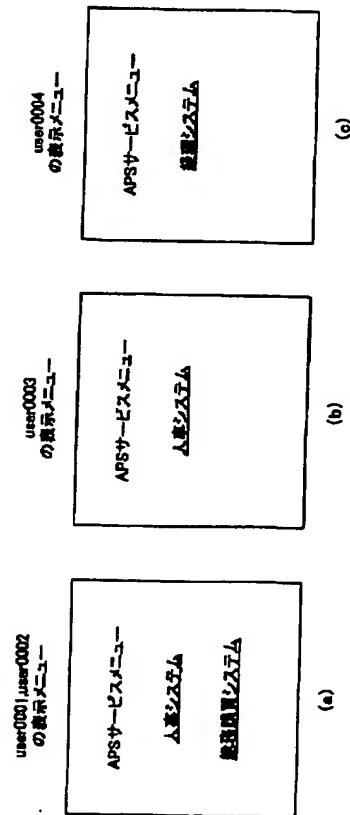
【図7】

ログイン画面の表示例を示す図

ログイン	
ユーザー名	パスワード
<input type="text"/>	<input type="text"/>
<input type="button" value="OK"/>	<input type="button" value="キャンセル"/>

【図8】

表示メニューの表示例を示す図



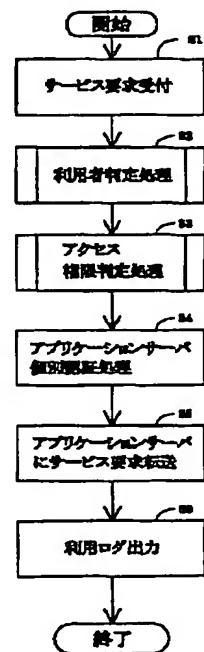
【図4】

利用者グループ情報定義データの構造

利用者	グループ名
user0001	group001
user0002	group001
user0003	group002
user0004	group003
:	:

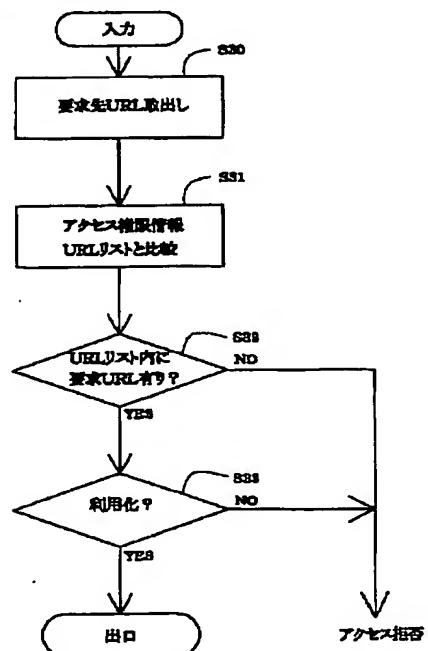
【図10】

中継サーバの初回のサービス要求受付から
アプリケーションサービスの提供開始までの
処理を示すフローチャート



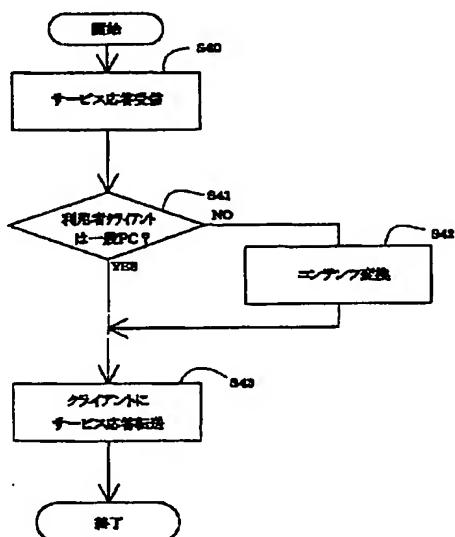
【図12】

図10のアクセス権限判定処理の詳細を示すフローチャート



【図13】

中継サーバがアプリケーションサーバからサービス応答を受け取った際の処理を示すフローチャート



[図 5]

【图 1-4】

グループ単位でのアクセス権限情報定義データの構造

課金明細の例を示す図

グループ名	アクセス可能URL	アクセス不可能URL
user0001	www.foo.jp/sv0001-1 www.foo.jp/sv0002/d1	www.foo.jp/sv0002/d1
user0002	www.foo.jp/sv0001-2	
user0003	www.foo.jp/sv0002	
:		

利用者	人事システム	給与システム	総務システム	**	**
user001	200円	—	100円	..	300円
user002	200円	—	100円	..	300円
user003	200円	—	—	..	200円
user004	—	500円	—	..	500円
:	:	:	:

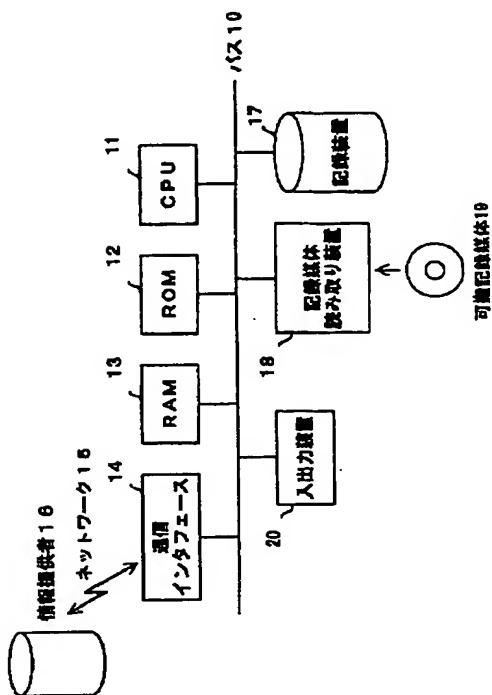
【図6】

アプリケーションサーバの 個別認証情報を示すデータ構造

個別認証情報		
利用者	サービス名	
user0001	総務購買システム	user=vp0001,password=xxxxxx,type=BASIC認証
user0002	総務購買システム	user=vp0002,password=yyyyyy,type=BASIC認証
:	:	:

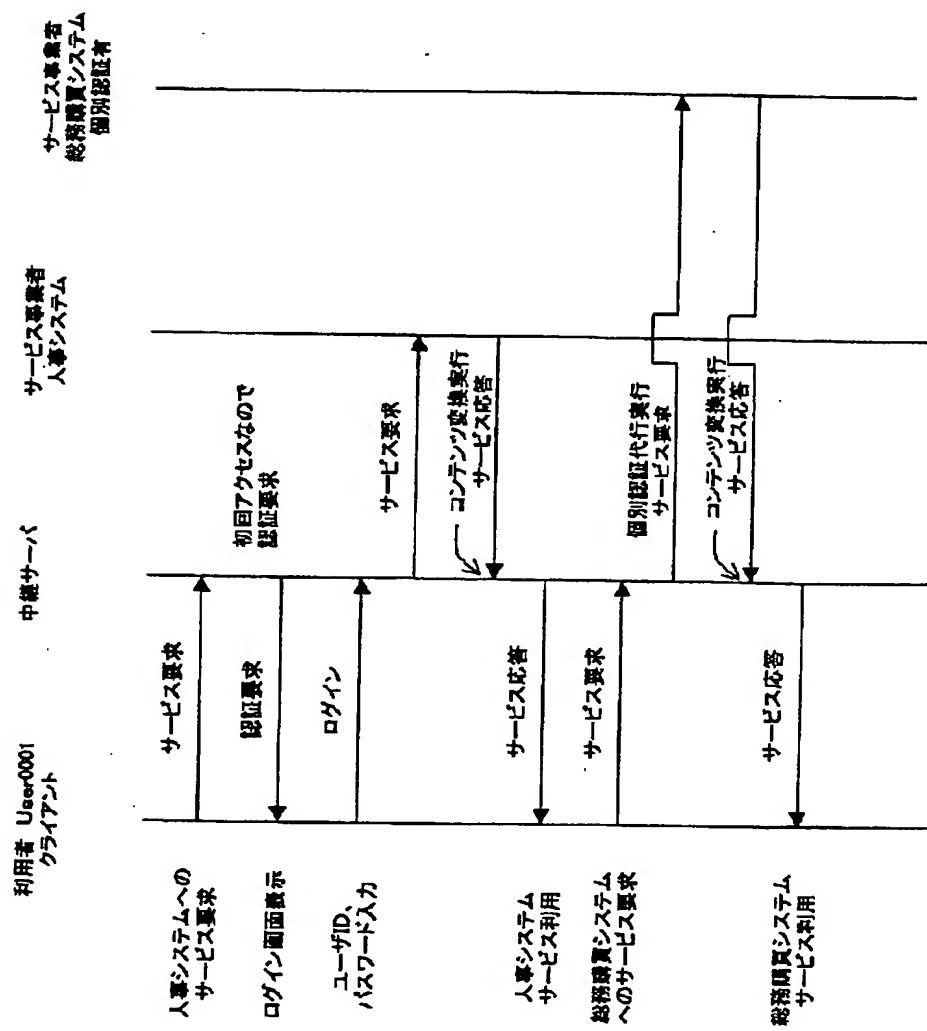
【図15】

本発明の実施形態の中端サーバ及び会員／課金管理サーバの機能をプログラムで実現しようとする場合に要求されるハードウェア環境の例を示す図



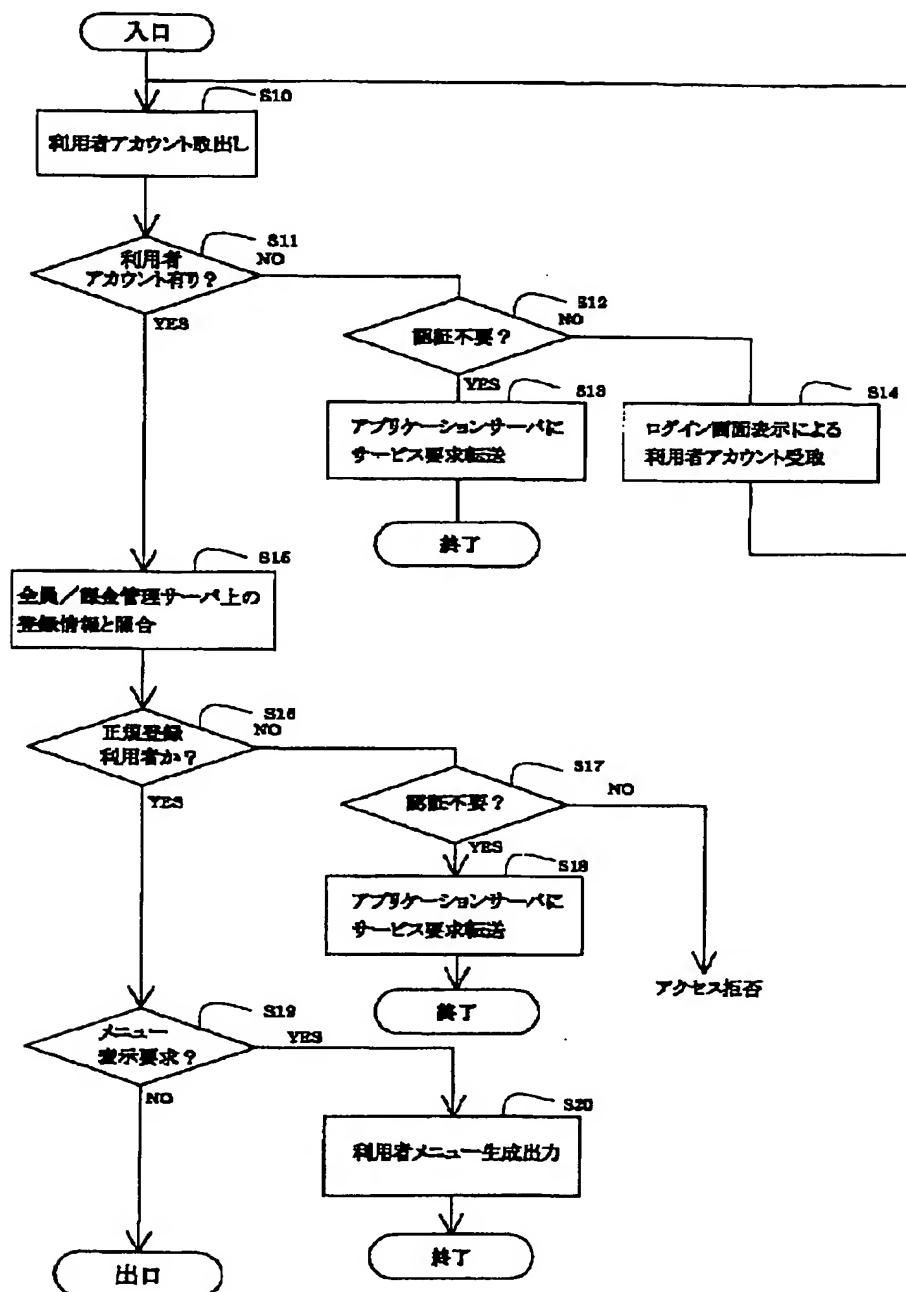
【図9】

ユーザが中継サーバを介してアプリケーションサーバに
サービス要求を行う場合のシーケンスを示す図



【図11】

図10の利用者判定の詳細を示すフローチャート



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.